Written Statement of
Donald (Andy) Purdy, Jr.
Director (Acting), National Cyber Security Division
Information Analysis and Infrastructure Protection Directorate
U.S. Department of Homeland Security

Committee on Science
United States House of Representatives

September 15, 2005

Good morning Chairman Boehlert and distinguished members of the Committee. My name is Andy Purdy, and I am the Acting Director of the Department of Homeland Security's National Cyber Security Division (NCSD). I am delighted to appear before you today to share with you the work of the NCSD and those with whom we are partnering to secure our national cyberspace and critical infrastructure. In my testimony today, I will provide an overview of NCSD, our operating mandates, our mission and goals, our priorities, and the programs in which we are engaged to meet those missions and goals.

DHS and Critical Infrastructure Protection

Over the course of the past several months Secretary Chertoff conducted a systematic evaluation of the Department's operations. On July 13th, Secretary Chertoff announced his six point agenda for the path ahead for the Department. As part of this agenda, the Secretary announced several Departmental organizational changes. Among these was the creation of a new Preparedness Directorate which would house a newly created office of the Assistant Secretary for Cyber Security and Telecommunications. Currently, cyber security is addressed by the NCSD, one of four divisions in the Office of Infrastructure Protection (IP), located within the Information Analysis and Infrastructure Protection Directorate.

In December 2003, President Bush issued Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection (HSPD-7), which established a national policy for federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks. Among other things, HSPD-7 identified 17[1] critical infrastructure and key resource sectors and assigned responsibility for each to a Sector Specific Agency (SSA), with DHS serving as the overall program coordinator.

[1]The NIPP identifies the following Critical Infrastructure Sectors and Key Resources: Food and Agriculture; Public Health and Healthcare; Drinking Water and Wastewater; Energy; Banking and Finance; National Monuments and Icons; Defense Industrial Base; Information Technology; Telecommunications; Chemical; Transportation Systems; Emergency Services; Postal and Shipping; Dams; Government Facilities; Commercial Facilities; Nuclear Reactors, Materials, and Waste.

Additionally, HSPD-7 set forth how DHS should address critical infrastructure protection, including "summary of activities to be undertaken in order to: define and prioritize, reduce the vulnerability of, and coordinate the protection of critical infrastructure and key resources."[2]

To meet this mandate, IP developed the National Infrastructure Protection Plan (NIPP), a plan that is to serve as the guide for addressing critical infrastructure and key resource protection. It sets forth a risk management framework for public and private sector stakeholders to work together to identify, prioritize, and conduct vulnerability assessments of critical assets and key resources in each sector. It also includes the identification of interdependencies of critical assets and key resources both within and across the sectors, as well as providing priority protective measures that owners and operators of such assets should undertake to secure them. Recognizing that more that 85 percent of the critical infrastructure is owned and operated by the private sector and that the development of public-private partnership is paramount to securing our nation's assets, private sector-led Sector Coordinating Councils (SCCs) are being established to work with their appropriate SSA via Government Coordinating Councils, which represent the government agencies that have a role in protecting the respective sectors.

Currently, the office of Infrastructure Protection is finalizing the NIPP and it is expected to be released later this year. This finalized document will refine the public-private partnership model and a process for protecting our critical infrastructures from physical or cyber attack or natural disasters.

DHS and Cyber Security

In June 2003, in response to the President's *National Strategy to Secure Cyberspace* and HSPD-7, the Department of Homeland Security created the NCSD as a national focal point for cyber security. The national strategy established the following five national priorities for securing cyberspace:

Priority I:	A National Cyberspace Security Response System
Priority II:	A National Cyberspace Security Threat and Vulnerability Reduction Program
Priority III:	A National Cyberspace Security Awareness and Training Program
Priority IV:	Securing Government's Cyberspace
Priority V:	National Security and International Cyberspace Security Cooperation

Given today's interconnected environment and DHS's integrated risk-based approach to critical infrastructure protection, NCSD's mission is to work collaboratively with public, private, and international entities to secure cyberspace and America's cyber assets. To meet that mission, NCSD developed a Strategic Plan that establishes a set of goals with specific objectives for each goal, and milestones associated with each objective. The Strategic Plan goals, which are closely aligned with the Strategy, HSPD-7, the NIPP, and the Cyber Annex to the National Response Plan, are as follows:

[2] Homeland Security Presidential Directive 7, December 17, 2003; http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html.

1. Establish a National Cyberspace Response System to prevent, detect, respond to, and reconstitute rapidly after cyber incidents;
2. Work with public and private sector representatives to reduce vulnerabilities and minimize severity of cyber attacks;
3. Promote a comprehensive awareness plan to empower all Americans to secure their own parts of cyberspace;
4. Foster adequate training and education programs to support the Nation's cyber security needs;
5. Coordinate with the intelligence and law enforcement communities to identify and reduce threats to cyberspace; and
6. Build a world class organization that aggressively advances its cyber security mission and goals in partnership with its public and private stakeholders.

To meet these goals, NCSD is organized into four operating branches to address the various aspects of the risk management structure: (1) U.S. Computer Emergency Readiness Team (US-CERT) Operations to manage the 24-7 threat watch, warning, and response capability that can identify emerging threats and vulnerabilities and coordinate responses to major cyber incidents; (2) Strategic Initiatives Branch to manage activities to advance cyber security in critical infrastructure protection, control systems security, software development, training and education, exercises, and standards and best practices; (3) Outreach and Awareness Branch to manage outreach, cyber security awareness, and partnership efforts to disseminate information to key constituencies and build collaborative actions with key stakeholders; and (4) Law Enforcement and Intelligence Branch to coordinate and share information between these communities and NCSD's other constituents in the private sector, public sector, academia, and others, and also to coordinate interagency response and mitigation of cyber security incidents. Together, these branches make up NCSD's framework to address the cyber security challenges across our key stakeholder groups and build communications, collaboration, and awareness to further our collective capabilities to detect, recognize, attribute, respond to, mitigate, and reconstitute after cyber attacks.

Cyber Security Priorities: Response and Risk Management

The Strategy, HSPD-7, and the NIPP provide NCSD with a clear operating mission and national coordination responsibility. To carry out this mission and its related responsibilities, NCSD has identified two overarching priorities: to build an effective national cyberspace response system and to implement a cyber risk management program for critical infrastructure protection. Our focus on these two priorities and related programs addresses the overarching NIPP Risk Management methodology and establishes the framework for securing cyberspace today and a foundation for addressing cyber security for the future.

Priority 1 – Cyber Incident Management: A National Cyberspace Response System

A core component of NCSD and our effort to establish a National Cyberspace Response System is the US-CERT Operations Center. US-CERT was established in September 2003 as a partnership between DHS and the public and private sectors to address cyber security issues. Building upon an initial partnership with the Computer Emergency Response Team Coordination

Center (CERT/CC) in Carnegie Mellon University's Software Engineering Institute, US-CERT now provides a national coordination center that links public and private response capabilities to facilitate information sharing across all infrastructure sectors and to help protect and maintain the continuity of our nation's cyber infrastructure. The overarching approach to this task is to facilitate and implement systemic global and domestic coordination of deterrence from, preparation for, defense against, response to, and recovery from cyber incidents and attacks across the United States, as well as from the cyber consequences of physical attacks or natural disasters.

US-CERT has four major programs of activity. First, US-CERT is DHS's 24-7-365 cyber watch, warning, and incident response center, and it provides coordinated response to cyber incidents, a web portal for secure communications with private and public sector stakeholders, including critical infrastructure owners and operators, a daily report, a public website (http://www.us-cert.gov/), and a National Cyber Alert System, which provides timely, actionable information to the public on both technical and non-technical bases. Second, US-CERT conducts malicious code analysis, provides malware technical support, and conducts cyber threat and vulnerability analysis. Third, US-CERT manages a situational awareness program and an Internet Health and Status service used by 50 government agency computer security incident response teams. Fourth, US-CERT manages programs for communication and collaboration among public agencies and key network defense service providers. In line with NCSD's close working relationship with NCS, US-CERT works closely with the National Coordinating Center for Telecommunications (NCC) to address and mitigate cyber threats including response and recovery. US-CERT also maintains a presence in the HSOC to ensure coordination throughout DHS.

As noted, NCSD has initiated a number of activities specifically to assist federal agencies in protecting their cyber infrastructure. NCSD established the Government Forum of Incident Response and Security Teams (GFIRST) to facilitate interagency information sharing and cooperation across federal agencies for readiness and response efforts. GFIRST is a group of technical and tactical practitioners of security response teams responsible for securing government information technology systems. The members work together to understand and handle computer security incidents and to encourage proactive and preventative security practices. The purpose of the GFIRST is to:

- Provide members with technical information, tools, methods, assistance, and guidance;
- Coordinate proactive liaison activities and analytical support;
- Further the development of quality products and services for the federal government;
- Share specific technical details regarding incidents within a trusted U.S. Government environment on a peer-to-peer basis; and
- Improve incident response operations.

GFIRST meets on a regular basis and held its first annual conference in April 2005 with more than 200 participants from federal, state, and local governments. The conference was a major success for US-CERT, and GFIRST has established further lines of communications across organizations. The technical workshops and speakers stimulated many technical interchanges regarding cyber first responder activities. In another step forward, GFIRST held its first

classified threat briefing with DHS Office of Information Analysis (IA), the Central Intelligence Agency, Department of Defense, and National Security Agency in June 2005.

US-CERT utilizes a secure collaboration platform, the US-CERT Portal, to support cyber information sharing and collaboration among the GFIRST community, and other cyber and critical infrastructure communities, such as the ISACs. The US-CERT Portal is being integrated into the Homeland Security Information Network (HSIN) and bridges the gap between the Government Coordinating Councils, the Sector Coordinating Councils, ISACs, and other private critical infrastructure information-sharing entities.

In addition to GFIRST, NCSD worked with the Department of Defense (DOD) and the Department of Justice (DOJ) to form the National Cyber Response Coordination Group (NCRCG) to provide a Federal Government approach to coordinated cyber incident response. NCSD created a Cyber Annex to the recently issued National Response Plan (NRP)[3] that provides a framework for responding to cyber incidents of national significance. As such, the Cyber Annex formalized the NCRCG as the principal federal interagency mechanism to coordinate preparation for, and response to, cyber incidents of national significance. The co-chairs of the NCRCG are DHS/NCSD, DOJ, and DOD. An additional 13 federal agencies with a statutory responsibility for and/or specific capability toward cyber security, including the intelligence community, comprise the membership. NCSD serves as the Executive Agent and point of contact for the NCRCG. The NCRCG has developed a concept of operations (CONOPS) for national cyber incident response that will be examined in the National Cyber Exercise, *Cyber Storm,* to be conducted by NCSD in November 2005, with public and private sector stakeholders.

The NCRCG is also reviewing capabilities of federal agencies from a cyber defense perspective to better leverage and coordinate the preparation for and response to significant cyber incidents. This effort will entail the following components:

- Mapping the current capabilities of government agencies related to cyber defense relative to detection and recognition of cyber activity of concern, attribution, response and mitigation, and reconstitution;
- Identifying capabilities within the government that US-CERT should leverage to maximize interagency coordination of cyber defense capabilities;
- Performing a gap analysis to identify the surge capabilities for possible leverage by, or collaboration with, the US-CERT for cyber defense issues in order to detect potentially damaging activity in cyberspace, to analyze exploits and warn potential victims, to coordinate incident responses, and to restore essential services that have been damaged; and
- Consider establishing formal resource sharing agreements with the other agencies per the cyber defense coordination needs identified through the process identified above.

An important element of a National Cyberspace Response System is our ability to address the global nature of cyberspace. Implementation of NCSD's international cyber security strategy

[3] http://www.dhs.gov/dhspublic/display?theme=15&content=4269

and its related outreach and collaboration objectives is well underway, as we participate in bilateral and multilateral outreach efforts and have established cooperative programs with key allies and countries of interest. Such international cooperation contributes to our overall global situational awareness and incident response capabilities in an area in which information moves at Internet speed and traditional borders do not apply.

With our efforts, accomplishments, and on-going programs, NCSD has made significant progress in managing cyber incidents and has taken substantial strides toward building a National Cyberspace Response System. We know there is more to do, and we are enhancing and evolving our readiness and response programs to further our efforts and address this dynamic environment.

Priority 2 – Cyber Risk Management: Assessing the Threat and Reducing the Risk

NCSD incorporated a risk management approach aligned with HSPD-7 and the resulting interim NIPP into its effort to better assess the threat and reduce the risk to our national cyberspace. Risk management includes risk assessment based on threat, vulnerabilities, and consequences, as well as efforts to reduce the risk by addressing vulnerabilities before an attack occurs, and mitigating and managing the consequences of a cyber attack that does occur. The NIPP risk management framework entails work with the intelligence community, law enforcement, and the private sector to better understand the cyber threat and a collaborative partnership between the private sector and federal, state, and local governments looking at people, cyber, and physical assets to identify and prioritize those assets, assess vulnerabilities, and coordinate the protection of critical infrastructure and key resources.

With regard to assessing the threat, NCSD collaborates with the law enforcement and the intelligence communities in a number of ways. DHS assisted in the coordination of cyber-related issues for the "National Intelligence Estimate (NIE) of Cyber Threats to the U.S. Information Infrastructure." The resulting classified document issued in February 2004 details actors (nation states, terrorist groups, organized criminal groups, hackers, etc.), capabilities, and intent (where known). In addition, NCSD has infused cyber requirements into the Standing Information Needs (SINs) and Priority Information Needs (PINs) for the intelligence community and continues to collaborate with them through IA to characterize cyber threats for accuracy. Finally, the NCRCG includes law enforcement and intelligence agencies and has working groups addressing botnets and attribution issues.

The private sector is also a resource for threat and risk related information, and NCSD works with its industry stakeholders to gather and communicate that information. The US-CERT Internet Health Service enables US-CERT to gather information from private sector resources regarding vulnerabilities, network attacks, and malicious code activity and provide that information to federal agencies. In addition, NCSD has identified preparedness and response as a key area of joint public-private effort and is working with the critical infrastructure sectors to identify attack/threat scenarios against which proactive protective measures can be taken and response plans can be developed. And, DHS utilizes the ISACs and critical sector elements of the HSIN to obtain and share cyber security information.

With regard to reducing the risk, DHS's SSA responsibilities under the NIPP include the Information Technology (IT) Sector and the Telecommunications Sector. Specifically, NCSD coordinates the IT Sector, and the National Communications System (NCS), another of the divisions in the IP directorate, coordinates the Telecommunications Sector. Reflecting the increasing convergence between these two communications sectors in today's market, NCSD and NCS work together closely to coordinate all efforts to protect the nation's critical cyber systems and the telecommunications transport layer.

The NIPP includes a cross-sector cyber responsibility for NCSD in addition to its IT Sector responsibility. The cross-sector responsibility is the collaborative effort between DHS/NCSD and the SSAs to ensure that deployed cyber elements have been secured in an appropriate and consistent manner across sectors. NCSD is responsible for providing cyber guidance to all sectors assisting them in understanding and mitigating cyber risk (including cyber infrastructure vulnerabilities) and in developing effective and appropriate protective measures. This guidance includes contributing cyber elements to the NIPP, reviewing the cyber aspects of the respective Sector Specific Plans (SSPs), and delivering cyber Critical Infrastructure Protection (CIP) training to SSAs to help them enhance the cyber aspects of their SSPs.

To implement these two NIPP Cyber elements, NCSD works with the Information Technology Information Sharing and Analysis Center (IT-ISAC) and the newly established Information Technology Sector Coordination Council (IT-SCC), as well as with the SSAs, ISACs and emerging SCCs in the other sectors.

In addition to NCSD's specific NIPP responsibilities, there are three major components to our cyber risk mitigation approach: the Internet Disruption Working Group (IDWG), the Control Systems Security Program, and the Software Assurance Program.

Protection of critical cyber assets goes hand-in-hand with protection of critical telecommunications assets; accordingly, NCSD and NCS are working closely together to collaborate on issues related to threats, identification of critical cyber assets, vulnerability and risk assessments, and development of appropriate protective measures that could be recommended for implementation by owners/operators. Within the NIPP framework, NCSD and NCS established the Internet Disruption Working Group (IDWG) in December 2004 to address the resiliency and recovery of Internet functions in case of a major cyber incident. The Department of Treasury and the Department of Defense are also engaged, and the working group is acting to extend the partnership to representatives from the private sector as well as international stakeholders. The IDWG reflects the convergence of telecommunications and information technology sectors in today's environment and the emergence of Next Generation Networks (NGN) that will compose the Internet of the future. An initial focus of the working group is to identify near term actions related to situational awareness, protection, and response that government and its stakeholders can take to better prepare for, protect against, and mitigate nationally significant Internet disruptions.

The interdependency between physical and cyber infrastructures is hardly more acute than in the use of control systems as integral operating components by many of our critical infrastructures. "Control Systems" is a generic term applied to hardware, firmware, communications, and

software used to perform vital monitoring and controlling functions of sensitive processes and enable automation of physical systems. Specific control systems used in the various critical infrastructure sectors include Supervisory Control and Data Acquisition (SCADA) systems, Process Control Systems (PCS), and Distributed Control Systems (DCS).

Examples of the critical infrastructure processes and functions that control systems monitor and control include energy transmission and distribution, pipelines, water and pumping stations, telecommunications, chemical processing, pharmaceutical production, rail and light rail, manufacturing, and food production. Increasingly, these control systems are implemented with remote access, open connectivity, and connections to open networks such as corporate intranets and the Internet. These sophisticated information technology tools are making our critical infrastructure assets more automated, more productive, more efficient, and more innovative, but they also may expose many of those physical assets to physical consequences from new, cyber-related threats and vulnerabilities.

To assure immediate attention is directed to protect these systems, NCSD established the Control Systems Security Program to coordinate efforts among federal, state, and local governments, as well as control system owners, operators, and vendors to improve control system security within and across all critical infrastructure sectors. As part of this Program, NCSD developed a Control Systems Strategy that incorporates five highly integrated goals to address the issues and challenges associated with control systems security. As such, our control systems activities support NCSD's overall efforts to address cyber security across critical infrastructure sectors over the long term, as well as the US-CERT's capability in the management, response, and handling of incidents, vulnerabilities, and mitigation of threat actions specific to critical control systems functions. NCSD also recognizes the significant attention being paid to PCS and SCADA security by various industry organizations in developing encryption standards, cryptography, modeling, and other tools to improve cyber security of control systems.

NCSD also established the US-CERT Control Systems Security Center (CSSC) in partnership with Idaho National Laboratory (INL) and other Department of Energy National Laboratories[4] in June 2004. The CSSC is involving other partners from control systems industry associations, universities, control systems vendors, and industry experts. Since its establishment, the CSSC has made considerable progress and some of its major accomplishments include:

- Established the US-CERT CSSC assessment and incident response facility located at INL and a US-CERT Support Operations Center for Control Systems;
- Established relationships with more than 25 potential industry partners and completed several agreements that established initial assessment, analysis, and vulnerability reduction plans within various industry sectors;
- Created the Critical Infrastructure Cyber Consequence Matrix to determine the industries of most concern, and a list of specific sites from the National Asset Database where Control Systems could cause a negative consequence due to failure or attack;

[4] Idaho (INL), Pacific Northwest (PNNL), Los Alamos (LANL), Argonne (ANL), Sandia (SNL), Savannah River (SRNL)

- Created a quantitative control systems cyber risk/decision analysis measurement methodology; and,
- Established the Process Control System Forum (PCSF) (in partnership with DHS's Science and Technology Directorate) with industry, academia, and government to accelerate the development of technology that will enhance the security, safety, and reliability of Control Systems, including legacy installations.

At the same time that the telecommunications and financial sectors have increased their dependence on information systems overall for information flows, service provision, and financial transactions, the energy, chemical, nuclear, food and agriculture, transportation, and water sectors have become increasingly dependent on process control systems for their critical operations. To more fully utilize the Matrix for analysis on the nature of consequences of attacks on the various sectors for risk management purposes, more information is needed about how these various sectors are using process control systems and the subsequent interdependencies.

Future FY05 and FY06 activities for NCSD's Control Systems Security Program include efforts to:

- Develop a comprehensive set of control systems security assurance levels for owners and operators;
- Sponsor government/industry workshops to increase awareness among control systems owners and operators of potential cyber incident impacts and vulnerabilities;
- Develop, populate, and validate control systems security scenario assessment tools to provide response teams a web-based application to assess impacts;
- Assess a minimum of three core systems and provide solutions to vulnerabilities and recommendations to protect against cyber threats; and
- Develop the US-CERT CSSC web page for information exchange.

The third major component of NCSD's cyber risk management program is our Software Assurance Program. Software is an essential component of the nation's critical infrastructure (power, water, transportation, financial institutions, defense industrial base, etc); however, defects in software can be exploited to launch cyber attacks as well as attacks against the critical infrastructure. NCSD developed a comprehensive software assurance framework that addresses people, process, technology, and acquisition throughout the software development lifecycle.

As part of the shared responsibility approach to cyber security, DHS is working to achieve a broader ability to routinely develop and deploy trustworthy software products. As such, DHS is shifting the security paradigm from "patch management" to "software assurance" by encouraging U.S. software developers to raise the bar on software quality and security. In collaboration with other federal agencies, academia, and the private sector, we are:

- Sponsoring the development of a repository of best practices and practical guidance for the software development community;
- Developing a software assurance common body of knowledge from which to develop curriculum for education and training;
- Examining recommendations from the Networking and Information Technology Research and Development (NITRD), Software Design and Productivity (SDP), and

High Confidence Software and Systems (HCSS) coordination groups and anticipating greater direct engagement with them in the future.
- Facilitating discussions with industry and academic institutions through Software Assurance Forums;
- Collaborating with NIST to inventory software assurance tools and measure effectiveness, identify gaps and conflicts, and develop a plan to eliminate gaps and conflicts;
- Completing the DHS/Department of Defense co-sponsored comprehensive review of the National Information Assurance Partnership (NIAP)[5] with the draft report to be published in September 2005; and
- Promoting investment in applicable software assurance research and development.

DHS will seek to reduce risks by raising the level of trust for all software, minimizing vulnerabilities and understanding threats. DHS will collaborate with government, industry, academic institutions, and international allies to achieve these software assurance objectives.

Another important cyber element of national infrastructure protection is the proliferation of the Internet in our society and daily lives. To mitigate the risks inherent in the rapidly growing user base and increasing usage, NCSD is engaged in a cyber security awareness program that leverages a variety of partners including the National Cyber Security Alliance, the Multi-State ISAC, and the Federal Trade Commission, among others, to reach out to the home user, K-12, small business, and higher education audiences to raise the American public's awareness of cyber risks and security measures.

Research and Development for Cyber Security and Critical Infrastructure Protection

Cyber-related research and development (R&D) is vital to improving the resiliency of the Nation's critical infrastructures. This difficult strategic challenge requires a coordinated and focused effort from across the Federal Government, state and local governments, the private sector, and academia to advance the security of critical cyber systems.

A critical area of focus for DHS is the development and deployment of technologies to protect the nation's cyber infrastructure, including the Internet and other critical infrastructures that depend on IT systems for their mission. Two components within DHS share responsibility for cyber R&D, with the Science & Technology (S&T) Directorate serving as the primary agent responsible for executing cyber security R&D programs. NCSD has responsibility for developing requirements for DHS' cyber security R&D projects.

The S&T Directorate's mission is to conduct, stimulate, and enable research, as well as to develop, test, evaluate, and transition homeland security capabilities to Federal, State and local

[5] The National Information Assurance Partnership, established in August of 1997, is a joint effort between NIST and NSA to provide technical leadership in security-related information technology test methods and assurance techniques. NIAP uses the Common Criteria to evaluate and certify commercial off the shelf (COTS) products. There has been much discussion in past years on the effectiveness (time and cost) of the NIAP process. As a result, the National Strategy to Secure Cyberspace recommended an independent review of the program be conducted to make recommendations for its improvement.

operational end-users. The goals of the DHS S&T Directorate's Cyber Security R&D program are to:

- Perform R&D aimed at improving the security of existing deployed technologies and to ensure the security of new emerging systems;
- Develop new and enhanced technologies for the detection of, prevention of, and response to cyber attacks on the nation's critical information infrastructure; and
- Facilitate the transfer of these technologies into the national infrastructure as a matter of urgency.

NCSD supports the overall DHS R&D mission by identifying areas for cyber innovation and coordinating with S&T. NCSD collects, develops, and submits cyber security R&D requirements to provide input to the federal cyber security R&D community and specifically to inform the DHS S&T Directorate's cyber security research priorities.

DHS S&T's Cyber Security Research and Development Center is currently working on several projects that support the recommendations of the National Strategy to Secure Cyberspace, while addressing the vulnerabilities of critical systems and infrastructures. The major areas are:

- Working with industry to develop secure routing protocols for the core of the Internet.
- Development of a cyber security test bed for researchers and developers.
- Establishment of a large database of anonymized data collected from the Internet to support research on new cyber security tools and techniques.
- Partnering with the government of Canada on a joint experiment involving the handheld BlackBerry data devices for secure communications between first responders.
- Funding research on understanding and countering emerging Internet threats.
- Funding small business innovative research in the development of new cyber security products.
- Coordination with the Institute for Information Infrastructure Protection (I3P) on the development of new technologies for securing SCADA systems and networks and analyzing the economics of cyber security.

To support and document cyber security R&D initiatives across the Federal Government, NCSD participates in the Cyber Security and Information Assurance Interagency Working Group (CSIA IWG), co-chaired by S&T and the Office of Science and Technology Policy (OSTP). Participants include the National Science Foundation (NSF), the Defense Advanced Research Projects Agency (DARPA), the National Institute of Standards and Technology (NIST) and many others. By reporting to both the Infrastructure Subcommittee and NITRD, the CSIA IWG is positioned to coordinate cyber security and information assurance R&D across agencies, while ensuring that the security of critical infrastructures is emphasized. The CSIA IWG is currently completing the Federal Cyber Security and Information Assurance R&D Plan.

Moving Forward

In connection with the National Infrastructure Protection Plan, efforts are underway to assess cyber threats, reduce vulnerabilities and identify significant interdependencies. These efforts will be fully implemented as the SSAs implement their portion of the NIPP. In partnership with

NCS and other agencies, we are working through the Internet Disruption Working Group to address the resiliency and recovery of Internet functions in the case of a major cyber incident. We have established a Control Systems Security Program to address core operating systems of critical infrastructure sectors. And, we are working with the government, private sector, and academia to promote the integrity and security of software. We continue to enhance our cyber incident readiness and response system, and we coordinate with our private sector stakeholders to provide protective guidance to our stakeholders through US-CERT. We are conducting a major exercise later this year to test the Cyber Annex to the National Response Plan. Through this effort, we will pull together appropriate entities in the Federal Government, state governments, and appropriate private sector stakeholders to test our capabilities and, subsequently, to improve our incident management process.

We are committed to achieving success in meeting our goals and objectives, but we cannot do it alone. We will continue to meet with industry representatives, our government counterparts, academia, and state representatives to formulate the partnerships needed for productive collaboration and leverage the efforts of all, so we, as a nation, are more secure in cyberspace and in our critical infrastructures.

Again, thank you for the opportunity to testify before you today. I would be happy to answer any questions you may have at this time.